Hindawi Publishing Corporation
International Journal of Mathematics and Mathematical Sciences
Volume 2013, Article ID 983607, 8 pages
http://dx.doi.org/10.1155/2013/983607

Hindawi

Research Article

Perpendicularity in an Abelian Group

Pentti Haukkanen,[1] Mika Mattila,[1] Jorma K. Merikoski,[1] and Timo Tossavainen[2]

[1] *School of Information Sciences, University of Tampere, 33014, Finland*
[2] *School of Applied Educational Science and Teacher Education, University of Eastern Finland, P.O. Box 86, 57101 Savonlinna, Finland*

Correspondence should be addressed to Pentti Haukkanen; pentti.haukkanen@uta.fi

Received 12 January 2013; Accepted 19 March 2013

Academic Editor: Petru Jebelean

We give a set of axioms to establish a perpendicularity relation in an Abelian group and then study the existence of perpendicularities in $(\mathbb{Z}_n, +)$ and $(\mathbb{Q}_+, \cdot)$ and in certain other groups. Our approach provides a justification for the use of the symbol $\perp$ denoting relative primeness in number theory and extends the domain of this convention to some degree. Related to that, we also consider parallelism from an axiomatic perspective.

1. Introduction

In [1, page 115], Graham et al. made the following suggestion:

When $\gcd(m, n) = 1$, the integers m and n have no prime factors in common and we say that they are *relatively prime*.

This concept is so important in practice, we ought to have a special notation for it; but alas, number theorists have not agreed on a very good one yet. Therefore we cry: HEAR US, O MATHEMATICIANS OF THE WORLD! LET US NOT WAIT ANY LONGER! WE CAN MAKE MANY FORMULAS CLEARER BY ADOPTING A NEW NOTATION NOW! LET US AGREE TO WRITE "$m \perp n$", AND TO SAY "m IS PRIME TO n," IF m AND n ARE RELATIVELY PRIME. Like perpendicular lines do not have a common direction, perpendicular numbers do not have common factors.

In fact, this cry had been answered even before it was made. Namely, in studying l-groups (i.e., groups with a lattice structure), Birkhoff [2, page 295] defines that two positive elements a and b of an l-group are disjoint if $a \wedge b = 0$ and uses the notation $a \perp b$ for disjoint elements. He also remarks that disjointness specializes to relative primeness in the l-group of positive integers.

A motivation for the present paper is to study how justified ultimately it is to use the symbol of perpendicularity to denote relative primeness. Does this practice rely only on the analogy between having no common direction and having no common factor or is there a deeper linkage to entitle this convention? This question leads us to ask which properties essentially establish the notion of perpendicularity in the algebraic context and what the most suitable algebraic context for the axiomatization of perpendicularity actually is; we have recently studied the axioms of perpendicularity from an elementary geometric point of view [3].

In an inner product space, perpendicularity obviously traces back to the inner product being zero. However, certain features of this perpendicularity can be shifted down to simpler algebraic structures. We will define perpendicularity in an Abelian group and examine it in Section 2. In Section 3, we will focus on perpendicularity in $(\mathbb{Z}_n, +)$. Davis [4] defined perpendicularity in an Abelian group differently. In Section 4, we will introduce his approach and compare it with ours. Thereafter, we will consider divisibility in $(\mathbb{Q}_+, \cdot)$ in Section 5 and parallelism in an Abelian group in Section 6. We will conclude our paper with a brief discussion and a supplement to the suggestion cited previously.

2. Axioms and Properties of Perpendicularity

Throughout this paper, $G = (G, +)$ is an Abelian group so that $G \neq \{0\}$. Unless otherwise stated, $\perp$ is a binary relation in G satisfying

(A1) $\forall a \in G : \exists b \in G : a \perp b$,

(A2) $\forall a \in G \setminus \{0\} : a \not\perp a$,

(A3) $\forall a, b \in G : a \perp b \Rightarrow b \perp a$,

(A4) $\forall a, b, c \in G : a \perp b \wedge a \perp c \Rightarrow a \perp (b + c)$,

(A5) $\forall a, b \in G : a \perp b \Rightarrow a \perp -b$.

We call $\perp$ a *perpendicularity* in G. This concept can be defined also in weaker structures by changing these axioms appropriately. For example, if G is an Abelian monoid, then we simply omit (A5). Since the *trivial perpendicularity*

$$x \perp y \Longleftrightarrow x = 0 \vee y = 0 \tag{1}$$

always exists, we are mainly interested in nontrivial perpendicularities.

We call $\perp$ *maximal* if it is not a subrelation of any other perpendicularity in G. There always exists a maximal perpendicularity. This is obvious if G is finite and, otherwise, it follows from Zorn's lemma.

Proposition 1 records some elementary properties of perpendicularity; we leave the proof for the reader.

Proposition 1. *Perpendicularity $\perp$ has the following properties:*

(a) $\forall a \in G : \ a \perp 0$,

(b) $\forall a \in G \setminus \{0\} : \ a \not\perp -a$,

(c) $\forall a, b_1, \ldots, b_k \in G, \gamma_1, \ldots, \gamma_k \in \mathbb{Z} : a \perp b_1, \ldots, b_k \Rightarrow a \perp (\gamma_1 b_1 + \cdots + \gamma_k b_k)$,

(d) $\forall a, b \in G, \mu, \nu \in \mathbb{Z} : a \perp b \Rightarrow \mu a \perp \nu b$.

The following characterization is useful in proving that a given relation is perpendicularity.

Proposition 2. *A binary relation $\perp$ in G is perpendicularity if and only if it satisfies (A1) and (A2) and*

(A6) $\forall a, b, c \in G : a \perp b \wedge a \perp c \Rightarrow (b - c) \perp a$.

Proof. The "only if"-part is trivial. To prove the "if"-part, we first show that our assumptions imply Proposition 1(a). Let $a \in G$. By (A1), there is $b \in G$ such that $a \perp b$. Putting $c := b$ in (A6) implies $0 \perp a$; in particular $0 \perp 0$. Further, (A6) with $a := 0$, $b := a$ and $c := 0$ gives $(a - 0) \perp 0$, that is, $a \perp 0$. Now we can verify the remaining axioms.

(A3) Assume $a \perp b$. Apply (A6) with $c := 0$; then $b \perp a$.

(A5) Assume $a \perp b$. Apply (A6) with $b := 0$ and $c := b$. Then $(-b) \perp a$, and so, by (A3), $a \perp -b$.

(A4) Assume $a \perp b$ and $a \perp c$; then $a \perp -c$ by (A5). Now (A6) with $c := -c$ implies $(b - (-c)) \perp a$, that is, $(b + c) \perp a$. Hence, by (A3), $a \perp (b + c)$. □

Is there a simple condition under which (A5) follows from (A1)–(A4)? The answer is positive.

Proposition 3. *If all elements of G have finite order and if $\perp$ satisfies (A1)–(A4), then it satisfies (A5). If G has at least one element of infinite order, then there exists a relation $\perp$ which satisfies (A1)–(A4) but not (A5).*

Proof. For the first part, assume that $a, b \in G$ satisfy $a \perp b$, and let the order of b be n. Then $a \perp (n - 1)b$ by (A4). But $(n - 1)b = -b$ and (A5) follows. For the second part, let $a \in G$ have infinite order. Then the subgroup $\{0, \pm a, \pm 2a, \ldots\}$ is isomorphic to $\mathbb{Z}$. The relation $\perp$ defined by

$$x \perp y \Longleftrightarrow \left(\exists \mu, \nu \in \mathbb{Z} : x = \mu a \wedge y = \nu a \wedge \mu\nu < 0\right) \vee x = 0 \vee y = 0 \tag{2}$$

satisfies (A1)–(A4) but not (A5). □

If $\emptyset \neq A \subseteq G$, we define the *perpendicular complement* or $\perp$-*complement* of A as follows:

$$A^{\perp} = \{y \in G \mid y \perp A\} = \bigcup_{G \supseteq B \perp A} B. \tag{3}$$

Here $y \perp A$ means that $y \perp x$ for all $x \in A$, and $B \perp A$ means that $y \perp A$ for all $y \in B$. Thus $A^{\perp}$ is the maximal set perpendicular to A. In particular, $G^{\perp} = \{0\}$ and $\{0\}^{\perp} = G$. We also define $\emptyset^{\perp} = G$.

Proposition 4. *If $A \subseteq G$, then $A^{\perp}$ is a subgroup of G. If G is cyclic, then $A^{\perp}$ is cyclic.*

Proof. The first part follows by applying the subgroup test and Proposition 2. The second part follows from the fact that any subgroup of a cyclic group is cyclic. □

The next theorem tells when G has a nontrivial perpendicularity.

Theorem 5. *The following conditions are equivalent:*

(a) *G has a nontrivial perpendicularity $\perp$,*

(b) *G has nontrivial cyclic subgroups H and K satisfying $H \cap K = \{0\}$,*

(c) *G has nontrivial subgroups H and K satisfying $H \cap K = \{0\}$.*

Proof. (a)⇒(b). Since $\perp$ is nontrivial, there exist $x, y \in G \setminus \{0\}$ such that $x \perp y$. Then $H = \langle x \rangle$ and $K = \langle y \rangle$ apply. Here $\langle a \rangle$ stands for the cyclic group generated by a.

(b)⇒(c). Trivial.

(c)⇒(a). Define $\perp$ by

$$x \perp y \Longleftrightarrow (x \in H \wedge y \in K) \vee (x \in K \wedge y \in H) \vee x = 0 \vee y = 0. \tag{4}$$

□

Next we consider the maximal perpendicularity in some examples of groups. In Examples 6–9, the group operation is addition.

Example 6. Let $G = \mathbb{Z}_6$. By Lagrange's theorem [5, page 130, Theorem 2], the smallest n such that $\mathbb{Z}_n$ has a nontrivial perpendicularity is $6 = 2 \cdot 3$ because n must have at least two different prime factors. The nontrivial subgroups of $\mathbb{Z}_6$ are $H = \langle 3 \rangle = \{0, 3\}$ and $K = \langle 2 \rangle = \{0, 2, 4\}$. Since $G = H \oplus K$,

it has exactly one nontrivial perpendicularity, defined by $0 \perp 0, 1, 2, 3, 4, 5$ and $3 \perp 2, 4$ and vice versa. Consequently, this perpendicularity is maximal.

Example 7. Let $G = \mathbb{Z}_2 \times \mathbb{Z}_2$, the Klein four group. Denote $0 = (0,0)$, $a = (0,1)$, $b = (1,0)$, $c = (1,1)$. The nontrivial subgroups are $A = \{0, a\}$, $B = \{0, b\}$, $C = \{0, c\}$. So, there are three nontrivial perpendicularities obtained as follows: Choose two elements of a, b, and c. Define that they are perpendicular to each other and to 0. Define that the remaining element is perpendicular to 0 only. All perpendicularities arising in this way are clearly maximal. We also note that $G = A \oplus B = B \oplus C = C \oplus A$.

Example 8. Let $G = \mathbb{Z}$. For each $n \geq 2$, the subgroup $\langle n \rangle = n\mathbb{Z}$ is nontrivial and there are no other nontrivial subgroups than those found in this way. Because $mn \in \langle m \rangle \cap \langle n \rangle$, there is no pair of nontrivial subgroups with intersection $\{0\}$. Hence G has only the trivial perpendicularity.

Example 9. Let $G = \mathbb{R}$. Since $\mathbb{R}$ has infinitely many pairs of nontrivial subgroups with intersection $\{0\}$, it has infinitely many nontrivial perpendicularities. For example, let $H = \mathbb{Q}$ and $K = \{x\sqrt{2} \mid x \in \mathbb{Q}\}$ and define $\perp$ by (4). To see that this perpendicularity is not maximal, let $H_1 = \{x\sqrt{3} \mid x \in \mathbb{Q}\}$ and $K_1 = \{x\sqrt{5} \mid x \in \mathbb{Q}\}$ and define $\perp'$ by

$$\begin{aligned} x \perp' y \Longleftrightarrow\ & (x \in H \wedge y \in K) \vee (x \in K \wedge y \in H) \\ & \vee (x \in H_1 \wedge y \in K_1) \vee (x \in K_1 \wedge y \in H_1) \\ & \vee x = 0 \vee y = 0. \end{aligned} \tag{5}$$

Then $x \perp y \Rightarrow x \perp' y$.

Example 10. Let $G = (\mathbb{Q}_+, \cdot)$, where $\mathbb{Q}_+$ denotes the set of positive rational numbers.

Every $c \in \mathbb{Q}_+$ can be uniquely expressed as

$$c = \prod_{p \in \mathbb{P}} p^{\nu_p(c)}, \tag{6}$$

where $\nu_p(c) \in \mathbb{Z}$ for each $p \in \mathbb{P}$ and only a finite number of them are nonzero. The symbol $\mathbb{P}$ stands for the set of primes. For example, if $c = 8/25$, then $\nu_2(c) = 3$, $\nu_3(c) = 0$, $\nu_5(c) = -2$, $\nu_7(c) = \nu_{11}(c) = \cdots = 0$.

Assign now

$$a \perp b \Longleftrightarrow \forall p \in \mathbb{P} : \nu_p(a) = 0 \vee \nu_p(b) = 0. \tag{7}$$

In other words, if

$$\begin{aligned} a = \frac{m}{u}, \quad b = \frac{n}{v}, \quad & m, u, n, v \in \mathbb{Z}_+, \\ & \gcd(m, u) = \gcd(n, v) = 1, \end{aligned} \tag{8}$$

then

$$a \perp b \Longleftrightarrow \gcd(mu, nv) = 1. \tag{9}$$

Hence, for example, $8/9 \perp 7/5$. In particular, for $m, n \in \mathbb{Z}_+$, applying (9) to $m/1$ and $n/1$ yields that

$$m \perp n \Longleftrightarrow \gcd(m, n) = 1. \tag{10}$$

So, it seems that Graham et al. were prophetically quite right with their suggestion—and not forgetting Birkhoff either! We will discuss the perpendicularity of positive rational numbers in more detail in Section 5.

3. Perpendicularity in $\mathbb{Z}_n$

Studying perpendicularities requires that we know the structure of G. Next we take a more thorough look at perpendicularity in $\mathbb{Z}_n$. To that end, we begin by introducing a suitable notation to discuss the structure of $\mathbb{Z}_n$ and record two lemmas which are useful in the search for the maximal perpendicularity. We will also use the notations introduced in Theorem 11 and the following lemmas throughout the next sections.

Theorem 11. *If*

$$n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}, \tag{11}$$

where $p_1, \ldots, p_r \in \mathbb{P}$ are distinct and $\alpha_1, \ldots, \alpha_r > 0$, then

$$\mathbb{Z}_n = H_1 \oplus \cdots \oplus H_r, \tag{12}$$

where

$$H_i = \langle e_i \rangle, \quad e_i = \frac{n}{p_i^{\alpha_i}}, \quad i = 1, \ldots, r. \tag{13}$$

The decomposition (12) *is unique (up to the order of subgroups).*

Proof. The claim (12) follows from [5, page 399, Corollary 1] and from the facts that $\mathbb{Z}_{p_i^{\alpha_i}} \cong H_i$ and $H_i \cap H_j = \{0\}$ for all $i, j = 1, \ldots, r$, $i \neq j$. Uniqueness follows from [5, page 399, Corollary 2]. □

Although we consider $\mathbb{Z}_n$ mainly as an Abelian group, it is now useful to work with $\mathbb{Z}_n$ as a ring.

Lemma 12. *For all $i, j = 1, \ldots, r$, $i \neq j$,*

$$e_i^2 \neq 0, \qquad e_i e_j = 0. \tag{14}$$

Proof. It is enough to consider $i = 1$, $j = 2$. Regarding e_1 and e_2 as integers, we have

$$\begin{aligned} e_1^2 &= \frac{n^2}{p_1^{2\alpha_1}} = p_2^{2\alpha_2} \cdots p_r^{2\alpha_r} \not\equiv 0 \pmod{n}, \\ e_1 e_2 &= \frac{n}{p_1^{\alpha_1}} \frac{n}{p_2^{\alpha_2}} \\ &= p_2^{\alpha_2} \cdots p_r^{\alpha_r} p_1^{\alpha_1} p_3^{\alpha_3} \cdots p_r^{\alpha_r} \\ &= p_3^{\alpha_3} \cdots p_r^{\alpha_r} n \equiv 0 \pmod{n}, \end{aligned} \tag{15}$$

and (14) follows. □

Lemma 13. *Let $\perp$ be a perpendicularity in $\mathbb{Z}_n$. Then*

$$\forall a, b, c, d \in \mathbb{Z}_n : a \perp b \Longrightarrow ca \perp db. \tag{16}$$

Proof. Let $c = \gamma 1$, $d = \delta 1$, where γ and δ are integers with $0 \le \gamma,\ \delta < n$. Since $ca = (\gamma 1)a = \gamma(1a) = \gamma a$ and, similarly, $db = \delta b$, Proposition 1(d) implies (16). □

Now we are ready to introduce a perpendicularity which turns out to be maximal in $\mathbb{Z}_n$. Let

$$x = x_1 + \cdots + x_r, \qquad y = y_1 + \cdots + y_r \in \mathbb{Z}_n, \tag{17}$$

where $x_i, y_i \in H_i$, $i = 1, \ldots, r$. The relation $\perp_0$, defined in $\mathbb{Z}_n$ by

$$x \perp_0 y \Longleftrightarrow \forall i \in \{1, \ldots, r\} : x_i = 0 \vee y_i = 0, \tag{18}$$

is clearly a perpendicularity.

Theorem 14. *The perpendicularity $\perp_0$ is maximal and every other perpendicularity in $\mathbb{Z}_n$ is contained in it.*

Proof. Let $\perp$ be another perpendicularity in $\mathbb{Z}_n$. Our claim is that $x \perp y \Rightarrow x \perp_0 y$. By (12), we can express

$$x = \xi_1 e_1 + \cdots + \xi_r e_r, \qquad y = \eta_1 e_1 + \cdots + \eta_r e_r, \tag{19}$$

where the integers $\xi_i, \eta_i \in \{0, \ldots, p_i^{\alpha_i} - 1\}$ and the residue class $e_i = n/p_i^{\alpha_i}$, $i = 1, \ldots, r$.

Suppose against the claim of theorem that there exist $x, y \in \mathbb{Z}_n$ such that $x \perp y$ but $x \not\perp_0 y$. Then $\xi_i, \eta_i \neq 0$ for some i. Reordering the indices so that $i = 1$ and applying (16), we have $xe_1 \perp ye_1$ which implies that

$$\xi_1 e_1^2 \perp \eta_1 e_1^2 \tag{20}$$

by (14). Hence, by Proposition 1(d),

$$\frac{\eta_1}{\gcd(\xi_1, \eta_1)} \xi_1 e_1^2 \perp \frac{\xi_1}{\gcd(\xi_1, \eta_1)} \eta_1 e_1^2, \tag{21}$$

that is,

$$\operatorname{lcm}(\xi_1, \eta_1)\, e_1^2 \perp \operatorname{lcm}(\xi_1, \eta_1)\, e_1^2. \tag{22}$$

Consequently, $\operatorname{lcm}(\xi_1, \eta_1)\, e_1^2 = 0$ by (A2). In other words, regarding also e_1 as an integer,

$$\begin{aligned} \operatorname{lcm}(\xi_1, \eta_1)\, e_1^2 &= \operatorname{lcm}(\xi_1, \eta_1)\, \frac{n^2}{p_1^{2\alpha_1}} \\ &= \operatorname{lcm}(\xi_1, \eta_1)\, p_2^{2\alpha_2} \cdots p_r^{2\alpha_r} \\ &\equiv 0 \pmod{n}, \end{aligned} \tag{23}$$

and $p_1^{\alpha_1}$ divides $\operatorname{lcm}(\xi_1, \eta_1)$. However, since it divides neither ξ_1 nor η_1, this is a contradiction. Hence, $x \perp_0 y$. □

Considering the direct sum (12) external, we can identify x and y in (17) with vectors $(x_1, \ldots, x_r)$ and $(y_1, \ldots, y_r)$, respectively. So, it is natural to define their "inner product" by

$$\langle x, y \rangle = x_1 y_1 + \cdots + x_r y_r. \tag{24}$$

Proposition 15 shows that this operation coincides with the ordinary multiplication in $\mathbb{Z}_n$.

Proposition 15. *Given $x, y \in \mathbb{Z}_n$,*

$$\langle x, y \rangle = xy. \tag{25}$$

Proof. We have

$$xy = \left(\sum_{i=1}^{r} x_i \right) \left(\sum_{i=1}^{r} y_i \right) = \sum_{i=1}^{r} x_i y_i + \sum_{\substack{i,j=1 \\ i \neq j}}^{r} x_i y_j. \tag{26}$$

But, recalling (19) and (14),

$$\sum_{\substack{i,j=1 \\ i \neq j}}^{r} x_i y_j = \sum_{\substack{i,j=1 \\ i \neq j}}^{r} \xi_i \eta_j e_i e_j = 0. \tag{27}$$

The claim follows. □

Theorem 16. *Let $\perp$ be a perpendicularity in $\mathbb{Z}_n$. Then*

$$\forall x, y \in \mathbb{Z}_n : x \perp y \Longrightarrow xy = 0. \tag{28}$$

Proof. If $x \perp y$, then $x \perp_0 y$ by Theorem 14. So, $xy = 0$ by (18) and (25). □

Does the converse of Theorem 16 hold if $\perp = \perp_0$? And, related to Proposition 15, is $\langle x, y \rangle = xy$ a proper inner product? Namely, an inner product in a real vector space is symmetric and bilinear and it satisfies $\langle x, x \rangle = 0 \Rightarrow x = 0$. The operation $\langle x, y \rangle = xy$ in $\mathbb{Z}_n$ has clearly the first and second properties but what about the third one? The answers to both questions are contained in Theorem 17.

Theorem 17. *The following conditions are equivalent:*

(a) $\alpha_1 = \cdots = \alpha_r = 1$,

(b) $\forall x, y \in \mathbb{Z}_n : xy = 0 \Rightarrow x \perp_0 y$,

(c) $\forall x \in \mathbb{Z}_n : x^2 = 0 \Rightarrow x = 0$.

Proof. (a)⇒(b). Assume that $x \not\perp_0 y$. Express x and y as in (19). We can rearrange the indices so that, for some $s \in \{1, \ldots, r\}$,

$$\begin{aligned} &\xi_i, \eta_i \neq 0, \quad i = 1, \ldots, s, \\ &\xi_i = 0 \vee \eta_i = 0, \quad i = s+1, \ldots, r. \end{aligned} \tag{29}$$

By (25),

$$xy = \xi_1 \eta_1 e_1^2 + \cdots + \xi_s \eta_s e_s^2. \tag{30}$$

If $\xi_1 \eta_1 e_1^2 + \cdots + \xi_s \eta_s e_s^2 = 0$, then the integer $\xi_1 \eta_1 e_1^2 + \cdots + \xi_s \eta_s e_s^2 \equiv 0 \pmod{n}$, that is,

$$\xi_1 \eta_1 \frac{n^2}{p_1^2} + \cdots + \xi_s \eta_s \frac{n^2}{p_s^2} \equiv 0 \pmod{n = p_1 \cdots p_r}. \tag{31}$$

However, this is impossible because none of $p_1, \ldots, p_s$ divides the left-hand side. (Namely, p_i divides every other summand except the ith one.) Therefore, $xy \neq 0$ and our claim follows by contradiction.

(b)⇒(c). If $x^2 = 0$, then $x \perp_0 x$ by (b) and $x = 0$ by (A2).

(c)⇒(a). Suppose that (a) does not hold. Then, say, $\alpha_1 > 1$. Let $x = n/p_1$. Since the integer

$$x^2 = \frac{n^2}{p_1^2} = \frac{p_1^{2\alpha_1} \cdots p_r^{2\alpha_r}}{p_1^2} = p_1^{2\alpha_1 - 2} p_2^{2\alpha_2} \cdots p_r^{2\alpha_r} \equiv 0 \pmod{n}, \tag{32}$$

the residue class $x^2 = 0$. But $x \neq 0$ and hence (c) does not hold. Again, our claim follows now by contradiction. □

Corollary 18. *If and only if the conditions of Theorem 17 are satisfied, then*

$$\forall x, y \in \mathbb{Z}_n : x \perp_0 y \Longleftrightarrow n \mid (xy), \tag{33}$$

where xy is the product of integers x and y.

Example 19. Let $G = \mathbb{Z}_{30}$. Since $30 = 2 \cdot 3 \cdot 5$, the decomposition (12) is

$$\mathbb{Z}_{30} = \left\langle \frac{30}{2} \right\rangle \oplus \left\langle \frac{30}{3} \right\rangle \oplus \left\langle \frac{30}{5} \right\rangle = \{0, 15\} \oplus \{0, 10, 20\} \oplus \{0, 6, 12, 18, 24\}. \tag{34}$$

For example, since $2 = 0 \cdot 15 + 2 \cdot 10 + 2 \cdot 6$ and $15 = 1 \cdot 15 + 0 \cdot 10 + 0 \cdot 6$, we have $2 \perp_0 15$. Generally, (33) implies that $x \perp_0 y$ if and only if the corresponding integers satisfy $30 \mid (xy)$.

Example 20. Let $G = \mathbb{Z}_{360}$. Since $360 = 2^3 \cdot 3^2 \cdot 5$, we have

$$\mathbb{Z}_{360} = \left\langle \frac{360}{2^3} \right\rangle \oplus \left\langle \frac{360}{3^2} \right\rangle \oplus \left\langle \frac{360}{5} \right\rangle = \{45, 90, \ldots, 315\} \oplus \{40, 80, \ldots, 320\} \oplus \{72, 144, \ldots, 288\}. \tag{35}$$

For example, $5 \perp_0 72$ because $5 = 1 \cdot 45 + 8 \cdot 40 + 0 \cdot 72$ and $72 = 0 \cdot 45 + 0 \cdot 40 + 1 \cdot 72$. Now (33) is only necessary for $\perp_0$ but not sufficient. For example, $10 \not\perp_0 36$ due to the fact that $10 = 2 \cdot 45 + 7 \cdot 40 + 0 \cdot 72$ and $36 = 4 \cdot 45 + 0 \cdot 40 + 3 \cdot 72$. However, $360 \mid (10 \cdot 36)$.

4. Another Definition of Perpendicularity

Davis [4] defined perpendicularity as a binary relation $\perp$ in G satisfying

(D1) $\forall a, b \in G : a \perp b \Rightarrow b \perp a$,

(D2) $\forall a \in G : 0 \perp a$,

(D3) $\forall a \in G : a \perp a \Rightarrow a = 0$,

(D4) $\forall a, b, c \in G : b \perp a \wedge c \perp a \Rightarrow (b + c) \perp a$,

(D5) $\forall a, b \in G : a \perp b \Leftrightarrow \{a\}^{\perp\perp} \cap \{b\}^{\perp\perp} = \{0\}$.

He assumes that G is an Abelian group, but the definition applies more generally to an Abelian monoid, too. It is easy to see that (D1)–(D4) are equivalent to (A1)–(A4). Axiom (D5) arises from introducing the concept of "disjointness" on a vector lattice; see [2, page 295], [6]. In fact, $\Leftrightarrow$ can be replaced with $\Leftarrow$ in (D5) due to the following observation.

Proposition 21. *Assume that $\perp$ satisfies (D1)–(D3) (or, equivalently, (A1)–(A3)). Then*

$$\forall a, b \in G : a \perp b \Rightarrow \{a\}^{\perp\perp} \cap \{b\}^{\perp\perp} = \{0\}. \tag{36}$$

Proof. We show first that if $\emptyset \neq A \subseteq G$, then

$$A \cap A^{\perp} = \{0\}. \tag{37}$$

If $x \in A \cap A^{\perp}$, then $x \perp y$ for all $y \in A$. In particular, $x \perp x$, and hence $x = 0$ by (D3) and (37) follows.

Assume next that $a \perp b$ and let $x \in \{a\}^{\perp\perp} \cap \{b\}^{\perp\perp}$. Since $x \perp \{b\}^{\perp}$ and $a \in \{b\}^{\perp}$, we have $x \perp a$ implying that $x \in \{a\}^{\perp}$. Thus $x \in \{a\}^{\perp} \cap \{a\}^{\perp\perp}$. But (37) applied to $A = \{a\}^{\perp}$ implies that $\{a\}^{\perp} \cap \{a\}^{\perp\perp} = \{0\}$ and $x = 0$ follows. □

How are these two perpendicularities related? We give a partial answer. Let us denote by A and D the axioms (A1)–(A5) and (D1)–(D5), respectively.

Proposition 22. *If all elements of G have finite order, then $D \Rightarrow A$. If G has at least one element of infinite order, then there exists a relation $\perp$ satisfying D but not A.*

Proof. The first claim follows from Proposition 3. Concerning the second one, $\perp$ defined by (2) establishes a relation satisfying D but not (A5). □

Proposition 23. *Assume that G has elements $a_1, a_2, a_3, a_4 \neq 0$ such that $\langle a_i \rangle \cap \langle a_j \rangle = \{0\}$ whenever $i \neq j$. Then there exists a relation $\perp$ satisfying A but not D.*

Proof. The relation $\perp$ defined by (5) with $H = \langle a_1 \rangle$, $K = \langle a_2 \rangle$, $H_1 = \langle a_3 \rangle$, and $K_1 = \langle a_4 \rangle$ satisfies A. Since $\{a_1\}^{\perp\perp} \cap \{a_3\}^{\perp\perp} = \langle a_1 \rangle \cap \langle a_3 \rangle = \{0\}$ and $a_1 \not\perp a_3$, it does not satisfy (D5). □

5. Divisibility in $\mathbb{Q}_+$

It will turn out that perpendicularity has got something to do also with divisibility in $\mathbb{Q}_+$. To that end, we begin by noticing that every $b \in \mathbb{Q}_+$ can be said to be a rational divisor of every $a \in \mathbb{Q}_+$ because $a = cb$ for some $c \in \mathbb{Q}_+$. So, this divisibility is trivial. In order to be able to discuss nontrivial divisibilities in $\mathbb{Q}_+$, we have to consider which properties essentially establish this relation. The following three ones seem quite obvious.

Let $\mid$ be a relation in $\mathbb{Q}_+$ satisfying

(i) $\forall a \in \mathbb{Q}_+ : a \mid a$,

(ii) $\forall a, b, c \in \mathbb{Q}_+ : c \mid a \wedge c \mid b \Rightarrow c \mid (ab)$,

(iii) $\forall a, b, c \in \mathbb{Q}_+ : c \mid b \wedge b \mid a \Rightarrow c \mid a$.

We call $\mid$ a *divisibility* in $\mathbb{Q}_+$. In other words, divisibility is a reflexive and transitive relation (i.e., a preorder) satisfying (ii).

If $b \mid a$, then we say that b is a *divisor* of a and that a is *divisible* by b. If $d \mid a, d \mid b$ and $c \mid a \wedge c \mid b \Rightarrow c \mid d$, then d is a *greatest common divisor* of a and b, denoted by $\gcd_{\mid}(a,b)$. All these notions are meaningful also in any Abelian monoid.

Let us recall that every $c \in \mathbb{Q}_+$ can be expressed as

$$c = \prod_{p\in\mathbb{P}} p^{\nu_p(c)}, \tag{38}$$

where $\nu_p(c) \in \mathbb{Z}$ for each $p \in \mathbb{P}$, and only a finite number of them are nonzero. If $\nu_p(c) \neq 0$, then p is a *prime factor* of c.

Consider the set S of all sequences $(n_2, n_3, \ldots, n_p, \ldots)$, where the index runs through $\mathbb{P}$, each $n_p \in \mathbb{Z}$, and only a finite number of them are nonzero. The mapping

$$f(c) = \left(\nu_2(c), \nu_3(c), \ldots, \nu_p(c), \ldots\right) \tag{39}$$

is an isomorphism from $(\mathbb{Q}_+, \cdot)$ onto $(S, +)$ where addition is defined termwise. For example,

$$\begin{aligned} f(45) + f\left(\frac{8}{25}\right) &= (0,2,1,0,0,\ldots) + (3,0,-2,0,0,\ldots) \\ &= (3,2,-1,0,0,\ldots), \\ f\left(45\cdot\frac{8}{25}\right) &= f\left(\frac{72}{5}\right) = f\left(2^3\cdot 3^2\cdot 5^{-1}\right) \\ &= (3,2,-1,0,0,\ldots). \end{aligned} \tag{40}$$

Given $a, b \in \mathbb{Q}_+$, we define their "inner product" being the Euclidean inner product of the vectors $f(a)$ and $f(b)$:

$$\langle a,b\rangle = \langle f(a), f(b)\rangle = \sum_{p\in\mathbb{P}} \nu_p(a)\,\nu_p(b). \tag{41}$$

Since only a finite number of summands are nonzero, this sum is finite. For example,

$$\left\langle 45, \frac{8}{25}\right\rangle = 0\cdot 3 + 2\cdot 0 + 1\cdot(-2) + 0 + 0 + \cdots = -2. \tag{42}$$

Next we define $|c|$ by setting $\nu_p(|c|) = |\nu_p(c)|$ for all $p \in \mathbb{P}$ or, equivalently, $|c| = f^{-1}((\nu_2(|c|), \nu_3(|c|), \nu_5(|c|), \ldots))$. For example, if $c = 40/63 = 2^3 \cdot 3^{-2} \cdot 5^1 \cdot 7^{-1}$, then $|c| = 2^3 \cdot 3^2 \cdot 5^1 \cdot 7^1 = 2520$. Letting $\perp_1$ be the same relation as the one defined by (7), it can be characterized now by

$$a \perp_1 b \Longleftrightarrow \langle |a|, |b|\rangle = 0. \tag{43}$$

Also the relation $\perp_2$ in $\mathbb{Q}_+$, defined by

$$a \perp_2 b \Longleftrightarrow \langle a,b\rangle = 0, \tag{44}$$

is a perpendicularity.

We will introduce one more nontrivial perpendicularity using divisibility. For that purpose, we first notice that the relation δ defined by

$$b\delta a \Longleftrightarrow \forall p \in \mathbb{P} : \nu_p(b) \le \nu_p(a) \tag{45}$$

is a divisibility, $\gcd_\delta(a,b)$ exists and is unique for all $a, b \in \mathbb{Q}_+$, and

$$\gcd_\delta(a,b) = \prod_{p\in\mathbb{P}} p^{\min(\nu_p(a),\nu_p(b))}. \tag{46}$$

Assume now that $m, n, u, v \in \mathbb{Z}_+$ so that $\gcd(m,u) = \gcd(n,v) = 1$. An alternative expression for (45) is

$$\frac{n}{v}\,\delta\,\frac{m}{u} \Longleftrightarrow n \mid m\wedge u \mid v, \tag{47}$$

and that for (46) is

$$\gcd_\delta\left(\frac{m}{u}, \frac{n}{v}\right) = \frac{\gcd(m,n)}{\operatorname{lcm}(u,v)}. \tag{48}$$

For example, if $a = 45/14 = 2^{-1}\cdot 3^2\cdot 5^1\cdot 7^{-1}$ and $b = 33/100 = 2^{-2}\cdot 3^1\cdot 5^{-2}\cdot 11^1$, then $\gcd_\delta(a,b) = 2^{-2}\cdot 3^1\cdot 5^{-2}\cdot 7^{-1} = 3/700$. Alternatively,

$$\gcd_\delta(a,b) = \frac{\gcd(45,33)}{\operatorname{lcm}(14,100)} = \frac{3}{700}. \tag{49}$$

Since $\gcd_\delta(|m/u|, |n/v|) = \gcd(mu, nv)$, we have by (9)

$$a \perp_1 b \Longleftrightarrow \gcd_\delta(|a|, |b|) = 1. \tag{50}$$

This relation generalizes (10) and answers the cry of Graham et al. in a slightly wider context than what they, perhaps, had thought.

Eugeni and Rizzi [7, Section 2] defined divisibility in $\mathbb{Q}_+$ by setting the relation γ so that

$$\frac{n}{v}\,\gamma\,\frac{m}{u} \Longleftrightarrow n \mid m\wedge v \mid u. \tag{51}$$

Then $\gcd_\gamma(a,b)$ always exists and is unique, and

$$\gcd_\gamma\left(\frac{m}{u}, \frac{n}{v}\right) = \frac{\gcd(m,n)}{\gcd(u,v)}. \tag{52}$$

For example,

$$\gcd_\gamma\left(\frac{45}{14}, \frac{33}{100}\right) = \frac{\gcd(45,33)}{\gcd(14,100)} = \frac{3}{2}. \tag{53}$$

We define now the corresponding perpendicularity by writing

$$\begin{aligned} a \perp_{\mathrm{ER}} b &\Longleftrightarrow \gcd_\gamma(a,b) = 1 \\ &\Longleftrightarrow \gcd(m,n) = \gcd(u,v) = 1. \end{aligned} \tag{54}$$

Summing up, we have at least three nontrivial perpendicularities in $\mathbb{Q}_+$. Let us see how they relate to one another.

$\perp_1$ *versus* $\perp_2$. Clearly $\perp_1 \Rightarrow \perp_2$ (i.e., $x\perp_1 y \Rightarrow x\perp_2 y$). The converse does not hold. For example, $6\perp_2 2/3$ but $6 \not\perp_1 2/3$.

$\perp_1$ *versus* $\perp_{\mathrm{ER}}$. Clearly $\perp_1 \Rightarrow \perp_{\mathrm{ER}}$. The converse does not hold. For example, $2/3 \perp_{\mathrm{ER}} 3/2$ but $2/3 \not\perp_1 3/2$.

$\perp_2$ *versus* $\perp_{\mathrm{ER}}$. These perpendicularities are independent. For example, $6\perp_2 2/3$ but $6 \not\perp_{\mathrm{ER}} 2/3$. On the other hand, $2/3 \perp_{\mathrm{ER}} 3/2$ but $2/3 \not\perp_2 3/2$.

However, regarding $(\mathbb{Z}_+, \cdot)$ as a submonoid of $(\mathbb{Q}_+, \cdot)$, it is obvious that $\perp_1 = \perp_2 = \perp_{\mathrm{ER}}$ in $\mathbb{Z}_+$. Moreover, in $\mathbb{Z}_+$, they yield the very perpendicularity proposed by Graham et al.

6. Parallelism

Parallelism is closely related to perpendicularity. Considering different geometric contexts we notice soon that, in general, parallelism does not have any other properties except those of equivalence. However, any equivalence relation cannot be said to stand for parallelism in any reasonable way. This leads us to ask whether it is possible or not to define parallelism in Abelian groups having a perpendicularity so that it makes sense.

Let G have a perpendicularity $\perp$ and let $a, b \in G$. We say that a and b are *parallel* and write $a \parallel b$ if $\{a\}^{\perp} = \{b\}^{\perp}$. The relation $\parallel$ is clearly an equivalence. If $a \neq 0$, then $a \nparallel 0$, since $\{0\}^{\perp} = G$ by Proposition 1(a) but $\{a\}^{\perp} \neq G$ by (A2). All nonzero elements are parallel if and only if $\perp$ is trivial.

If $G = \mathbb{Z}_n$ and $\perp = \perp_0$, then, recalling (19),

$$\begin{aligned} x \parallel y &\Longleftrightarrow \left(\forall i \in \{1, \ldots, r\} : \xi_i = 0 \Longleftrightarrow \eta_i = 0\right) \\ &\Longleftrightarrow \{x\}^{\perp} = \{y\}^{\perp} = H_{i_1} \oplus \cdots \oplus H_{i_t}, \end{aligned} \tag{55}$$

where $\xi_i = \eta_i = 0 \Leftrightarrow i \in \{i_1, \ldots, i_t\}$. For example, consider $\mathbb{Z}_{30}$ (see Example 19). Since $2 = 0 \cdot 15 + 2 \cdot 10 + 2 \cdot 6$ and $16 = 0 \cdot 15 + 1 \cdot 10 + 1 \cdot 6$, we have $\{2\}^{\perp} = \{16\}^{\perp} = \{0, 15\}$, and so $2 \parallel 16$.

Now, let $G = \mathbb{Q}_+$ and let $\perp_1$, $\perp_2$, and $\perp_{\mathrm{ER}}$ be as before. Denote the corresponding parallelisms by $\parallel_1$, $\parallel_2$, and $\parallel_{\mathrm{ER}}$, respectively. Then $a \parallel_1 b$ if and only if a and b have the same prime factors. Further, $m/u \parallel_{\mathrm{ER}} n/v$ if and only if m and n have the same prime factors and u and v have the same prime factors.

Let us study how these parallelisms relate to one another.

$\parallel_1$ *versus* $\parallel_2$. We show that $\parallel_2 \ \Rightarrow \ \parallel_1$. Assume first that $a \parallel_2 b$. If $a \nparallel_1 b$, then there exists $p_0 \in \mathbb{P}$ such that, say, $\nu_{p_0}(a) = 0$ and $\nu_{p_0}(b) \neq 0$. But now $p_0 \perp_2 a$ and $p_0 \not\perp_2 b$, and so $\{a\}^{\perp_2} \neq \{b\}^{\perp_2}$ contradicting the assumption. The converse does not hold. For example, let $a = 6$ and $b = 12$; then $a \parallel_1 b$. If $x = 2/3$, then $x \perp_2 a$ but $x \not\perp_2 b$, and hence $\{a\}^{\perp_2} \neq \{b\}^{\perp_2}$. In other words, $a \nparallel_2 b$.

$\parallel_1$ *versus* $\parallel_{\mathrm{ER}}$. Clearly $\parallel_{\mathrm{ER}} \ \Rightarrow \ \parallel_1$. The converse does not hold. For example, $2/3 \parallel_1 3/2$ but $2/3 \nparallel_{\mathrm{ER}} 3/2$.

$\parallel_2$ *versus* $\parallel_{\mathrm{ER}}$. We show that $\parallel_2 \ \Rightarrow \ \parallel_{\mathrm{ER}}$. Given $p_1, \ldots, p_t \in \mathbb{P}$, denote by $N(p_1, \ldots, p_t)$ the set of such positive integers that are not divisible by any p_i, $i = 1, \ldots, t$. Let $a = m/u \in \mathbb{Q}_+$, $\gcd(m, u) = 1$. Factorize

$$m = p_1^{\alpha_1} \cdots p_h^{\alpha_h}, \qquad u = q_1^{\beta_1} \cdots q_k^{\beta_k}, \tag{56}$$

where $p_1, \ldots, p_h, q_1, \ldots, q_k \in \mathbb{P}$ are distinct and $\alpha_1, \ldots, \alpha_h, \beta_1, \ldots, \beta_k > 0$. (If $m = 1$ or $u = 1$, then the corresponding "empty product" is one.) Now

$$\begin{aligned} \{a\}^{\perp_2} = \Bigg\{ & \frac{p_1^{\xi_1} \cdots p_h^{\xi_h}}{q_1^{\eta_1} \cdots q_k^{\eta_k}} \frac{x}{y} \mid \alpha_1 \xi_1 + \cdots + \alpha_h \xi_h + \beta_1 \eta_1 \\ & + \cdots + \beta_k \eta_k = 0, \\ & x, y \in N(p_1, \ldots, p_h, q_1, \ldots, q_k) \Bigg\}. \end{aligned} \tag{57}$$

(The "empty sum" is zero.) Assume that $b = n/v \in \mathbb{Q}_+$, $\gcd(n, v) = 1$, satisfies $a \parallel_2 b$, that is, $\{a\}^{\perp_2} = \{b\}^{\perp_2}$. Then, by (57), necessarily

$$n = p_1^{\rho_1} \cdots p_h^{\rho_h}, \qquad v = q_1^{\sigma_1} \cdots q_k^{\sigma_k}, \tag{58}$$

where $\rho_1, \ldots, \rho_h, \sigma_1, \ldots, \sigma_k > 0$. Hence $a \parallel_{\mathrm{ER}} b$, and the claim follows. The converse is not valid. For example, $2/3 \parallel_{\mathrm{ER}} 4/3$ but $2/3 \nparallel_2 4/3$.

7. Discussion

This paper began with a citation by three established mathematicians and computer scientists who showed a remarkable intuition by promoting the use of the symbol of perpendicularity in number theory. Indeed, we have previously seen how this notion settles comfortably in this setting and gains new meanings at a more general level in the context of Abelian group theory. We conclude this paper with the following supplement to their proposal.

Let perpendicularity and parallelism mean here $\perp_1$ and $\parallel_1$, respectively. Consider the "direction vector" of $c \in \mathbb{Q}_+$ by $(c(2), c(3), \ldots, c(p), \ldots)$, where $c(p) = 0$ if $\nu_p(c) = 0$ and $c(p) = 1$ otherwise. For example, the direction vectors of $45, 1$, and $8/25$ are, respectively $(0, 1, 1, 0, 0, \ldots)$, $(0, 0, \ldots)$, and $(1, 0, 1, 0, 0, \ldots)$.

Now, like the directions of perpendicular lines are as different as possible, the prime factors of perpendicular (positive rational) numbers are as different as possible; that is, such numbers do not have common prime factors. In other words, the direction vectors of perpendicular numbers are as different as possible in the sense that they have no common element of value one. Like parallel lines have the same direction, parallel numbers have the same prime factors. In other words, their direction vectors are equal.

Finally, we note that perpendicularity can be axiomatized in a natural way also in many other algebraic structures. Davis [8] did that in a ring. In a vector space, perpendicularity is customarily defined based on an inner product. Another possible approach is to supplement (A1)–(A5) with suitable axioms concerning the multiplication of a vector by a scalar. It might be interesting to study under which additional conditions there exists an inner product inducing this perpendicularity.

Acknowledgment

The authors would like to thank the referees for carefully reading the paper and kind comments.

References

[1] R. L. Graham, D. E. Knuth, and O. Patashnik, *Concrete Mathematics: A Foundation for Computer Science*, Addison-Wesley, Reading, Mass, USA, 2nd edition, 1994.

[2] G. Birkhoff, *Lattice Theory*, American Mathematical Society, Providence, RI, USA, 3rd edition, 1993.

[3] P. Haukkanen, J. K. Merikoski, and T. Tossavainen, "Axiomatizing perpendicularity and parallelism," *Journal for Geometry and Graphics*, vol. 15, no. 2, pp. 129–139, 2011.

[4] G. Davis, "Orthogonality relations on abelian groups," *Journal of the Australian Mathematical Society. Series A*, vol. 19, pp. 173–179, 1975.

[5] W. K. Nicholson, *Introduction to Abstract Algebra*, John Wiley & Sons, New York, NY, USA, 2nd edition, 1999.

[6] A. I. Veksler, "Linear spaces with disjoint elements and their conversion into vector lattices," *Leningradskiĭ Gosudarstvennyĭ Pedagogičeskiĭ Institut imeni A. I. Gercena. Učenye Zapiski*, vol. 328, pp. 19–43, 1967 (Russian).

[7] F. Eugeni and B. Rizzi, "An incidence algebra on rational numbers," *Rendiconti di Matematica*, vol. 12, no. 3-4, pp. 557–576, 1979.

[8] G. Davis, "Rings with orthogonality relations," *Bulletin of the Australian Mathematical Society*, vol. 4, pp. 163–178, 1971.